Remarks

1. Summary of Office Action

In the Office Action mailed on February 2, 2004, the Examiner rejected claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, and 36 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,999,629 (Heer et al., hereinafter "Heer"). Further, the Examiner rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34 under 35 U.S.C. § 103(a) as being obvious over a combination of Heer and U.S. Patent No. 4,731,840 (Minszewski et al., hereinafter "Mniszewski"), and claims 10 and 22 as being obvious over a combination of Heer and U.S. Patent No. 5,124,117 (Tatebayashi et al., hereinafter "Tatebayashi").

2. Amendments

In the specification, the first full paragraph on page 19 has been amended to correct a typographical error.

In the claims, Applicants have amended independent claims 1, 13, 25, and 31 to recite the invention more clearly, as fully supported by Applicants' specification. Applicants have also amended claims 26, 27, 29, and 30 to correct typographical errors.

Pending in this application are claims 1-36, of which claims 1, 13, 25, and 31 are independent and the remainder are dependent.

3. Response to § 102 Rejections

As noted above, the Examiner rejected claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, and 36 under 35 U.S.C. § 102(e) as being anticipated by Heer.

Under M.P.E.P. § 2131, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. Applicants respectfully traverse the rejections of claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-

32, and 36 because Heer does not disclose or suggest each and every element of any one of these claims.

Applicants' claimed invention is directed to a method and system for network security. In this regard, each of independent claims 1, 13, 25, and 31, as amended above, recites in various ways the limitations of (i) using security determined by a first key material for communications between a first and second network devices, *the first key material including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using security determined by a second key material (that includes a second base key) for communications between the second and a third network devices, *wherein the security determined by the first key material is stronger than the security determined by the second key material.* (*See* Applicants' amendments above for how amended claims 1, 13, 25, and 31 presently recite these limitations in way or another).

Claims 2, 5, 8, 9, 14, 17, 20, 21, 26, 30, 32, and 36 depend from respective claim 1, 11, 25, or 31, and therefore incorporate all of the elements of claim 1, 11, 25, or 31.

Heer discloses a method and system for managing the secrecy of encryption keys, such as those used to encrypt/decrypt programs in a Video-On-Demand (VOD) system. According to Heer, in the VOD system, an Information Protection System (ICS) provides a program encryption key to an Access Control System (ACS), which, in turn, distributes the program encryption key to a subscriber terminal requesting the program associated with the encryption key. (*See* Heer, e.g., at col. 4, lines 16-29). As taught by Heer, to protect the secrecy of program encryption keys exchanged between two system entities, the program encryption keys can be encrypted using a symmetrical key that is shared between the two entities.

For example, in the VOD system described in Heer, an ICS security module shares a symmetrical key with an ACS security module. When the ICS security module is to communicate a program encryption key to the ACS security module, the ICS security module encrypts the program encryption key with the ICS/ACS shared symmetrical key. In a similar way, when the ACS security module is to provide the program encryption key with to a particular subscriber terminal (security) module, the ACS security module encrypts the program encryption key with a symmetrical key that it shares with the particular subscriber terminal module.

But, Applicants do not find in Heer any disclosure of at least the limitations of (i) using security determined by a first key material for communications between a first and a second network device, *the first key material including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using security determined by a second key material (that includes a second base key) for communications between the second and a third network device, *wherein the security determined by the first key material is stronger than the security determined by the second key material*, as recited, in one way or another, in each of Applicants' claims.

Rather, Heer discloses a system, in which three system devices (e.g., the ICS, the ACS, and the subscriber terminal as described above) communicate with each other using respective shared symmetrical keys. In the Office Action, the Examiner proposed the ICS to be a first network device, the ACS to be a second network device, and the subscriber terminal to be a third network device. Further, the Examiner asserted that the symmetrical key shared between the ICS security module and the ACS security module "is generated by the public encryption key and the private key (key extension) of the information processing system", and further, "the security module of the access control system (second network device) and the subscriber the subscriber (third network device) may share a respective symmetrical key (second key material) that will be unique to the pair as a result of the public key associated with the security module of the subscriber module (third network device) and a per-use randomly generated key (key extension) emanating from the access control system security module."

The Examiner's assertion that Heer discloses a key extension is incorrect. The symmetrical key shared by the ICS security module and the ACS security module in Heer is merely generated *as a function* , i.e., specific function CV = f (PK_{id}^{S} mod p), of the public encryption key PK_{id} and the private key S_{id}, rather than being provided in the form of a base key and a key extension as asserted by the Examiner. (Also *see* Heer, at col. 5, lines 30-64, for a complete explanation of how the ICS/ACS shared symmetrical key is generated).

In fact, a person of ordinary skill in the art would logically understand that forming the ICS/ACS key in the manner taught by Heer is not the same as providing a first key material that includes a base key and that also includes a key extension in addition to the base key, as presently claimed by Applicants and also clearly illustrated in Applicants' specification.

Moreover, Applicants respectfully submit that Heer remains silent as to a degree of security used for communications between a first network device and a second network device, and between the second network device and a third network device. In particular, Applicants do not find in Heer any description of the claimed limitation of (i) using security determined by a first key material for communications between a first and second network devices and (ii) using security determined by a second key material for communications between the second and a third network devices, *wherein the security determined by the first key material is stronger than the security determined by the second key material.*

Advantageously, with Applicants' claimed invention, the presence of a key extension in the first key material allows the first and second network devices to communicate using stronger security, while the lack of a key extension in the second key material prevents the second and third network devices from implementing stronger security.

Because Heer fails to teach all of the limitations of any of claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, and 36, Heer fails to anticipate these claims under 35 U.S.C. § 102.

4. Response to § 103 Rejections

As noted further noted above, rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24 under 35 U.S.C. § 103(a) as being obvious over a combination of Heer and Mniszewski, and claims 10 and 22 as being obvious over a combination of Heer and Tatebayashi.

a. Claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24

The Examiner rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34 on grounds of obviousness over the combination of Heer and Mniszewski.

In order to establish a *prima facie* case of obviousness of a claimed invention by applying a combination of references, the prior art must teach or suggest all of the claim limitations. M.P.E.P. § 2143. Applicants respectfully traverse the rejections of claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24, because the combination of Heer and Mniszewski fails to disclose or suggest every element of any of claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34.

Each of claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24 depends from respective claim 1, 11, 25, or 31 and therefore incorporates the limitations of claim 1, 13, 25, or 31. As discussed above, Heer fails to teach the invention of any of claims 1, 13, 25, and 31. Therefore, Heer also fails to teach or suggest the invention as recited in any of claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24. Further, Applicants respectfully submit that Mniszewski fails to overcome the deficiencies of Heer described above.

Applicants do not concede that the representations made more specifically by the Examiner with respect to dependent claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 24 are correct. However, Applicants submit that those other points are moot in view of the fact that the cited combination fails to teach or suggest the invention as recited in any of independent claims 1, 13, 25, and 31.

b. Claims 10 and 22

Next, the Examiner rejected claims 10 and 22 on grounds of obviousness over the combination of Heer and Tatebayashi.

As noted above, in order to establish a *prima facie* case of obviousness of a claimed invention by applying a combination of references, the proposed combination must teach or suggest all of the elements of the claimed invention. Applicants respectfully traverse the rejections of claims 10 and 22, because the combination of Heer and Tatebayashi fails to disclose or suggest the invention as recited in any of these claims.

Claim 10 ultimately depends from claim 1 and therefore incorporates all of the elements of claim 1. Claim 22 ultimately depends from claim 13 and therefore incorporates all of the elements of claim 13. As discussed above, Heer fails to teach or suggest the invention as recited in claims 1 and 13. Therefore, Heer fails to teach or suggest the invention as recited in each of claims 10 and 22. Further, Applicants respectfully submit that Tatebayashi fails to overcome the deficiencies of Heer described above.

Applicants do not concede that the representations made more specifically by the Examiner with respect to dependent claims 10 and 22 are correct. However, Applicants submit that those other points are moot in view of the fact that the cited combination fails to teach or suggest the invention as recited in independent claims 1 and 13.

5. Comments on the Allowable Subject Matter

The Examiner stated that claims 11, 12, 23, 24, 29, and 35, objected to as being dependent upon a rejected base claim, would be allowable if rewritten in independent from including all of the limitations of the base claim and any intervening claims. As explained above, Applicants submit that base claims 1, 13, 25, and 35 are patentably distinguishable over Heer. Consequently, Applicants submit that claims 11, 12, 23, 24, 29, and 35 are in condition for allowance as is, and that no amendment should be required.

6. Conclusion

Accordingly, Applicants respectfully submit that all of the presently pending claims 1-35 are in condition for allowance, and Applicants respectfully request favorable reconsideration.

Respectfully submitted,

McDONNELL BOEHNEN
HULBERT & BERGHOFF

Date: June 2, 2004

By: Joanna Skyles

Joanna Skyles
Reg. No. 54,454